

Remarks

Applicants have carefully considered the Office Action dated January 27, 2005 and the references cited therein. Applicants respectfully request reexamination and reconsideration of the application.

Applicants respectfully traverse the rejection of claim 19-20 under 35 USC section 101 as being directed to nonstatutory subject. For a considerable time now the USPTO has allowed claims in the form of "a computer data signal embodied in a carrier wave", the theory being that if computer program product claims are allowable why should the nature of the medium, i.e. tangible or intangible, make any difference. A search of the publicly accessible portion of the USPTO database (www.uspto.gov) reveals that multiple United States patents issued since 1976 have issued in this form. Typical examples can be seen in the following US Patents and their respective claims:

6,112,240	Claims 38-48
6,131,121	Claim 12
6,182,279	Claims 21-32
6,185,184	Claim 14-16
6,356,914	Claims 19-25

In light of the foregoing, if the examiner still has questions the examination guidelines published by the USPTO should be consulted.

Claims 1-20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over a non-patent a publication entitled "How to Set up the Paladin E-mail Client", www.circa.ufl.edu/handouts/softdist/pladin/paladin.html, pp. 1-6, August 18, 1997, hereafter "Paladin Systems", in view of a publication by Crocker, D., Standard for the Format of ARPA Internet Text Messages, RFC-822, IETF, pp. 1-39, August 13, 1982, hereafter "RFC-822", and PGP for Personal Privacy, v. 5.5, User Guide, Network Associates, Inc., pp. 1-150, 1998, hereafter "PGP for Personal Privacy", and the Admitted Prior Art, hereafter APA.

Applicants traverses the rejection of claims 1 - 20 under 35 U.S.C. §103(a) on the grounds that the Examiner has failed to create a *prima facie* case of obviousness. In accordance with MPEP §2143.03, to establish a *prima facie* case of obviousness 1) the prior art reference (or references when combined) must teach or suggest *all* of the claim limitations; 2) there must be some suggestion or motivation to modify a reference or combine references; and 3) there must be a reasonable expectation of success.

In setting forth the rejections, regarding claim 1, the Examiner expressly admits that Paladin System does not teach a system that (1) inserts an encryption flag in a header associated with an electronic message/e-mail; (2) places the header and the plain text message in an outbox; (3) when the sender is online, in response to the flag, requests the digital certificate from the mail system; and (4) uses the received certificate to encrypt the plain text mail message. Essentially, the Examiner is admitting that Paladin System does not teach any of the specific recited limitations. Instead the Examiner is relying on RFC-822, alleging that it teaches an e-mail message with an encryption flag in the header (pp. 16 and 21) and further asserting that it would have been obvious to one of ordinary skill in the art at the time the invention was made to have the Paladin System implement e-mail message formats according to the RFC standard, thereby including an encrypted flag in the e-mail message because use of the encrypted flag would indicate to the recipient that the message was encrypted, thereby allowing the recipient of the message to decrypt the message.

Applicants traverse such rejection for the following reasons. The Examiner has alleged that the encryption field (RFC-822, page 21) is analogous to the encryption flag, as claimed. Applicants respectfully disagree with the Examiner's analogy. Specifically, the encryption field identifies that the associated message *is encrypted* and contains a first data word used to identify the software used to encrypt the message, and an optional, second data word to aid the recipient in selecting the proper decryption key. Conversely, the encryption flag of the present invention is used to indicate that the electronic message *is not encrypted*. As opposed to the identifier of the encryption type and a code word of the encryption field of RFC-822. Accordingly, the Examiner can appreciate that the implementation and function of the encryption flag is not analogous to, and, therefore, fundamentally different from, the encryption field of RFC-822.

Accordingly, Applicants respectfully traverse the rejection of claim 1 on the grounds that the Examiner has failed to show how the prior art reference teach or suggest *all* of the claim limitations.

In addition, Applicants traverse the rejection of claim 1 on the grounds that the Examiner has not provided some suggestion, teaching or motivation to combine the teachings of Paladin System and RFC-822 and that such references are not properly combinable. The examiner will note that the stated motivation for combining the Paladin System and RFC-822 references , i.e., including an encrypted flag in the e-mail message because use of the encrypted flag would indicate to the recipient that the message was encrypted, thereby allowing the recipient of the message to decrypt the message, is neither an object or motivation of the present invention nor part of the problems solved by the claimed method.

Notwithstanding the Examiner's attempted combination of Paladin System with RFC-822, the Examiner expressly admits that the attempted combination still does not teach a method in that (2) places the header and the plain text message in an outbox; (3) when the sender is online, in response to the flag, requests the digital certificate from the mail system; and (4) uses the received certificate to encrypt the plain text mail message. Essentially, the Examiner is admitting that the Examiner's attempted combination of Paladin System with RFC-822 teaches only (1) inserting an encryption flag in a header associated with an electronic message/e-mail. Instead the Examiner is relying on the PGP for Personal Privacy to teach the other limitations, alleging that it teaches how some e-mail agents encrypt e-mail messages after they are placed in an outbox and before the messages are sent and further asserting that it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine PGP for Personal Privacy's teaching regarding the encryption of e-mail at the time the message is sent with the method of the combination of the Paladin System in view of RFC-822 by having the method encrypt the sent e-mail message after the user goes back online because of PGP for Personal Privacy's express teaching that some e-mail systems operate in this manner (p. 52). The Examiner further alleges that in the resulting combination, the method would move queued to send e-mail into the outbox when the sender goes online and then encrypt the e-mail message.

Applicants further traverse the rejection of claim 1 on the grounds that the Examiner has not provided some suggestion, teaching or motivation to combine the teachings of all three of Paladin System, RFC-822 and PGP for Personal Privacy and that such references are not properly combinable. The examiner will note that there is no stated motivation for combining the three of Paladin System, RFC-822 and PGP for Personal Privacy. How can examiner reconcile the alleged teachings of PGP for Personal Privacy, in which a queued email message is not yet encrypted, with the alleged combined teachings of Paladin System and RFC-822, in which the encryption field of the message header indicates that the message has not only been encrypted, but the type of encryption and a code word to assist in decryption?

Notwithstanding the Examiner's attempted combination of Paladin System in view of RFC-822 and PGP for Personal Privacy, the Examiner still expressly admits that the attempted combination does not teach a method that (3) requests a digital certificate from the mail system; and (4) uses the received certificate to encrypt the plain text mail message. Essentially, the Examiner is admitting that the Examiner's attempted combination of PGP for Personal Privacy with the combined Paladin System/RFC-822 teaches only (2) places the header and the plain text message in an outbox. Instead, the Examiner is again relying on the PGP for Personal Privacy publication alleging that it teaches a method in which when an e-mail message sender does not have a recipient's certificate and public key, that information is requested from a key server (pp. 45-46). The Examiner further asserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine PGP for Personal Privacy's teaching regarding the retrieval of a certificate from a key server with the method of the combination of the Paladin System in view of RFC-822 by having the e-mail agent request a locally unavailable certificate from a key server because of PGP for Personal Privacy's explicitly teaching that these are alternative ways of getting keys/certificates (p. 45). The Examiner further alleges that in the resulting combination, the method of the combination of the Paladin System in view of RFC-822 and PGP for Personal Privacy, the certificate used to encrypt the e-mail message comes from a key server as opposed to the mail system.

The Examiner still further alleges that in light of the subject applications, disclosure of the Lotus Notes system – an integrated groupware system that combines, among other things, an e-mail server and a directory server that provides X.509 certificates (pp. 2-3), it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of the combination of the Paladin System in view of RFC-822 and PGP for Personal Privacy to use an integrated e-mail system and key server as taught by the Lotus Notes system, and , that this modification would have been obvious because an integrated software solution makes the software provider responsible for the integration of the components, thus reducing the administration burden on the purchaser of the software.

In response, Applicants traverse the rejection of claims under 35 U.S.C. §103(a) on the grounds that the Examiner has failed to create a *prima facie* case of obviousness since the Examiner has not provided some suggestion, teaching or motivation to combine all of the teachings of the Paladin System, RFC-822, PGP for Personal Privacy and APA that such references are not properly combinable. The Examiner has failed to disclose where in any of Paladin System, RFC-822, PGP for Personal Privacy, and APA there is a teaching, suggestion or motivation to combine the respective teachings of *all four* references, as required for a *prima facie* case of obviousness. The Examiner has, cited and combined, in piece-meal manner, the current combination Paladin System, RFC-822, PGP for Personal Privacy, and APA. In light of the admitted deficiencies in the respective references, alleging that Paladin System can be combined with RFC-822, and that PGP for Personal Privacy can be combined with the combination of Paladin System/ RFC-822, and, still further that APA can be combined with the combination of Paladin System/ RFC-822/ PGP for Personal Privacy is not the same as providing a teaching, suggestion or motivation that the respective teachings of *all four* of Paladin System, RFC-822, PGP for Personal Privacy, and APA be combined in a manner in which there must be a reasonable expectation of success and which must teach or suggest *all* of the claim limitations.

By the own Examiner's admissions of record and for the same reasons as set forth above with respect to the traversal of the claim 1 rejections, Applicants respectfully assert that the Examiner has failed to show how the prior art references teach or

suggest *all* of the limitations of claim 1 and that the Examiner has further failed to disclose where in any of Paladin System, RFC-822, PGP for Personal Privacy, and APA there is a teaching, suggestion or motivation to combine the respective teachings of *all four* references, as required for a prima facie case of obviousness. Accordingly, claim 1 is believed allowable. Claims 2-6 include all the limitations of claim 1 and are likewise believed allowable over the combination of references for at least the same reasons as claim 11, as well as for the merits of their own respective limitations.

Claim 7 is directed to an apparatus for encrypting an electronic message composed by a sender using an abbreviated address book for delivery over a mail system and has been amended to specifically recite “the encryption flag indicating that the electronic message *is unencrypted*” (claim 7, lines 5-6, emphasis added). As stated previously, with regard to the traversal of the claim 1 rejections, Applicants respectfully disagree with the Examiner's analogy that the encryption field (RFC-822, page 21) is analogous to the encryption flag, as claimed. Specifically, the encryption field identifies that the associated message *is encrypted* and contains a first data word used to identify the encryption software. In claim 7, the encryption flag indicates that the electronic message *is unencrypted*. The Examiner can appreciate that the implementation and function of the encryption flag is not analogous to, and, therefore different from, the encryption field of RFC-822. Accordingly, claim 7 is believed allowable over the combination of cited references because the prior art reference (or references when combined) do not teach or suggest *all* of the claim limitations. Claims 8-12 include all the limitations of claim 7 and are likewise believed allowable for at least the same reasons as claim 7, as well as for the merits of their own respective limitations.

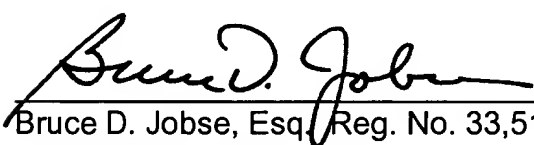
Claims 13 has been amended include limitations similar to claim 7 and is likewise believed allowable for at least the same reasons as claim 7, as well as for the merits of its own respective limitations (claim 13, lines 7-8). Claims 14-18 include all the limitations of claim 13 and are likewise believed allowable over the combination of references for at least the same reasons as claim 13, as well as for the merits of their own respective limitations.

Claim 19 is the computer and data signal counterparts to claim 13 and recites similar language (claim 19, lines 6-7) and is likewise believed allowable for at least the same reasons as claims 7 and 13, as well as for the merits of its own respective limitations. Similarly, claim 20 includes all the limitations of claim 19 and is likewise believed allowable over the combination of references for at least the same reasons as claim 19, as well as for the merits of its own respective limitations.

Applicants respectfully reassert all of the remarks and traversals set forth in prior responses to the extent still relevant to the outstanding rejections.

Applicants believe the claims are in allowable condition. A notice of allowance for this application is solicited earnestly. If the Examiner has any further questions regarding this amendment, he/she is invited to call Applicants' attorney at the number listed below. The Examiner is hereby authorized to charge any fees or credit any balances under 37 CFR §1.17, and 1.16 to Deposit Account No. DA-12-2158.

Respectfully submitted,



Date: 4/27/05

Bruce D. Jobse, Esq., Reg. No. 33,518
KUDIRKA & JOBSE, LLP
Customer Number 021127
Tel: (617) 367-4600 Fax: (617) 367-4656